

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
ABILENE DIVISION

UNITED STATES OF AMERICA

vs.

JASON ALAN SEYFFERT

§
§
§
§
§

CASE NO. 1:08-CR-057(01)

MOTION TO SUPPRESS AND BRIEF IN SUPPORT

TO THE HONORABLE JUDGE OF SAID COURT:

Now comes JASON ALAN SEYFFERT, Defendant, and files this Motion to Suppress and shows the following:

1. Defendant has been charged with the offense of Possession of Child Pornography.

2. On or about August 29, 2008, the Federal Bureau of Investigation, Taylor County Sheriff's Office, and other law enforcement executed a search warrant at the residence of Defendant. As a result of the execution of said search warrant, evidence that may be used by the State at trial of this cause was seized.

3. The actions of the Federal Bureau of Investigation, Taylor County Sheriff's Office, and other law enforcement violated the constitutional and statutory rights of the Defendant under the Fourth, Fifth, Sixth and Fourteenth Amendments to the United States Constitution.

4. JASON ALAN SEYFFERT was arrested without lawful warrant, probable cause or other lawful authority in violation of the rights of JASON ALAN SEYFFERT pursuant to the Fourth, Fifth, Sixth, and Fourteenth Amendments to the United States Constitution.

5. Any statements obtained from JASON ALAN SEYFFERT were obtained in violation of the rights of JASON ALAN SEYFFERT pursuant to the Fourth, Fifth, Sixth, and Fourteenth Amendments to the United States Constitution.

6. Any wire, oral, or electronic communications intercepted in connection with this case that were seized without lawful warrant, probable cause or other lawful authority in violation of state and federal law or the fruits thereof. The search of Mr. Seyffert's email conducted by America Online was conducted without probable cause or reasonable suspicion that a crime was committed.

7. Any tangible evidence and the fruits thereof seized in connection with this case was seized without warrant, probable cause or other lawful authority in violation of the rights of JASON ALAN SEYFFERT pursuant to the Fourth, Fifth, Sixth, and Fourteenth Amendments to the United States Constitution.

8. Defendant specifically shows that the search warrant at issue in this case, under which said evidence was seized, was in violation of the Fourth, Fifth, Sixth, and Fourteenth Amendments to the United States Constitution:

The warrant was illegally issued because probable cause on the supporting affidavit was tainted by an illegal search conducted by America Online. This illegal search was the sole basis of all further investigation and searches in this matter. Without the fruits of this illegal search Mr. McNoll's affidavit does not reflect sufficient probable cause to justify the issuance of a search warrant, in that: (i) the affidavit lacks sufficient underlying circumstances which would permit the conclusion that the alleged contraband was at the location in which it was claimed; and (ii) the affidavit fatally fails to state sufficient underlying circumstances to establish the credibility of the affiant.

9. Therefore, Defendant requests that the following matters be suppressed at trial of this cause:

a. Any and all tangible evidence seized by law enforcement officers or others in connection with the detention and arrest of JASON ALAN SEYFFERT in this case or in connection with the investigation of this case, and any testimony by the Federal Bureau of Investigation, Taylor County Sheriff's Office, and other Law enforcement or any other law enforcement officers or others concerning such evidence.

b. The arrest of JASON ALAN SEYFFERT at the time and place in question and any and all evidence which relates to the arrest, and any testimony by the Federal Bureau of Investigation, Taylor County Sheriff's Office, and other Law enforcement or any other law enforcement officers or others concerning any action of JASON ALAN SEYFFERT while in detention or under arrest in connection with this case.

c. All written and oral statements made by JASON ALAN SEYFFERT to any law enforcement officers or others in connection with this case, and any testimony by the Federal Bureau of Investigation, Taylor County Sheriff's Office, and other Law enforcement or any other law enforcement officers or others concerning any such statements.

d. All wire, oral, or electronic communications intercepted in connection with this case and any and all evidence derived from said communications.

e. Any other matters that the Court finds should be suppressed upon hearing of this motion.

I. ARGUMENT

The sole question is whether or not the search of Defendant's email by America Online constitutes sufficient state action to implicate Fourth Amendment Protection. The affidavit of Gary McNoll provides evidence of such action who states that internet service providers such as America Online are required to turn over information regarding the transmission of child pornography via email. Obviously, this is not possible unless some type of search is conducted by the internet service provider. In this case America Online used a computer program to conduct the search of Defendant's email absent any probable cause or reasonable suspicion to believe that defendant was committing a crime. See Affidavit of Gary McNoll attached hereto as **Exhibit "A"** and incorporated by reference as if fully set forth herein.

Additional discovery, and in all probability depositions, ought to be granted by the Court to determine the extent of state action in this case. The only evidence before the Court at this time is that America Online was forced to conduct the search.

This case is factually similar to *Maxwell v. United States*. *Maxwell v. United States*, 45 M.J. 406 (1996). In *Maxwell*, America Online conducted a search which was more expansive than the federal search warrant, including screen names, not used by subscribers named in the search warrant. *Id* at 420. The search was conducted on AOL's expectation as to what the warrant would actually request. *Id*.

One of these screen names not in the warrant searched by the AOL program was "Zirloc." The email transmissions from Zirloc were turned over to the Air Force Office of Special Investigations ("OSI"). *Id*. These files did not contain graphic images, but contained email transmissions to another junior Air Force officer known as "Launchboy", discussing the sexual orientation and sexual preferences of Defendant. The language contained in this email was relevant to Defendant's court-martial proceedings for conduct that, "disorders and neglects to the prejudice of good order and discipline in the armed forces," and brings discredit upon the armed forces." *Id* at 417, 420.

II. DEFENDANT HAS AN EXPECTATION OF PRIVACY IN HIS EMAIL

The Court found that the emails sent from Zirloc were the fruits of an unlawful search and must be excluded. To get there, the Court found that the expectation of privacy Defendant had in his emails invoked Fourth Amendment Protection. *Id* at 425. The Court further stated that the expectations of privacy depend on the type of email and the intended recipient. *Id*. The U.S. Navy-Marine Corps Court of Appeals and the Sixth Circuit Court of Appeals also concluded that Defendants have a legitimate expectation of privacy in their

emails. *United States v. Ohnesorge*, 60 M.J. 946 (2005); *United States v. Warshak*, 490 F.3d 455 (2007).

Additionally, having a contract with an Internet Service Provider does not eliminate one's expectation of privacy nor does the fact that Internet Service Providers routinely scan users' e-mails for viruses, spam, and child pornography. *Warshak v. U.S.*, 490 F.3d 455 (6th Cir. 2007). In this case, the contract was between Defendant's father and AOL. Defendant in no way consented to any search of his emails, account or electronic transmissions nor did Defendant know that any monitoring was occurring. Defendant believed that his emails would be viewed only by their intended recipient and had no reason to believe otherwise. See **Exhibit "B"** attached hereto and incorporated for all purposes.

III.

THE GOOD FAITH EXCEPTION DOES NOT RENDER THE SEARCH OF DEFENANT'S HOUSE LAWFUL

Like the *Maxwell* case, AOL's search was not in reliance on the precise language of the search warrant. *Id* at 426. In *Maxwell*, AOL was informed that a warrant was going to be issued and began gathering information they thought was relevant in support of the anticipated warrant. The results of the search AOL conducted in anticipation of the warrant were broader than that requested in the warrant, and the information turned over to the FBI exceeded the scope of the warrant.

In this case, AOL determined which records to turn over to the FBI, absent any probable cause, reasonable suspicion or search warrant. AOL believed turning over information was a requirement of federal law. See Affidavit of Gary McNoll attached hereto as **Exhibit "A"** and incorporated by reference as if fully set forth herein. The *Maxwell* Court refused to uphold admission of appellant's "Zirloc" transmissions based on the good faith exception to the warrant requirement because it was clear that the warrant was not relied upon in the search of the accounts.

In this case, the search from AOL occurred before the warrant was even issued so the good faith exception cannot apply as a matter of law and logical reasoning.

IV.

STATE ACTION

In *Maxwell*, the Government argued that records from the "Zirloc" account cannot be suppressed under the Fourth Amendment because the search by AOL was a private search. *Id* at 429. The Court disagreed with this argument applying the *Coolidge* Test to determine whether state action exists. In *Coolidge v. New Hampshire*, the Supreme Court stated that state action is found "if in light of all the circumstances of the case, [the private actor] must be regarded as having acted as an instrument' or agent of the state when she produced the challenged items." *Coolidge v. New Hampshire*, 403 U.S. 443 (1971). In *Maxwell*, as in this

case, AOL constructed the computer retrieval program prior to service of the warrant. *Id.* The *Maxwell* Court found state action because AOL gathered the evidence at the request of the Government, in anticipation of a warrant, and solely for the purpose of surrendering it to government authorities to satisfy the warrant. *Id.* In this case, two of these three reasons relied on by the *Maxwell* Court in finding state action exist. Here, AOL conducted a search because the law imposed a duty to turn over emails depicting child pornography, and the sole purpose for the search is compliance with federal law. Surely, AOL conducts this type of search not out of any sense of morality, as the primary purpose of AOL is profit, but because they fear civil or criminal liability if they do not.

IV. RELIEF SOUGHT

WHEREFORE, PREMISES CONSIDERED, Defendant prays that the Court allow Defendant sufficient time to collect evidence in support of Defendant's argument that the actions of America Online constituted State Action, grant an evidentiary hearing, and suppress such matters at trial of this cause, and for such other and further relief in connection therewith that is proper.

Respectfully submitted,

MEHAFFEY & WATSON
2441 South 1st Street
Abilene, Texas 79605
Tel: (325) 674-1900
Fax: (325) 674-1901

By: _____

Samuel Mehaffey
State Bar No. 24032857
Attorney for JASON ALAN SEYFFERT

CERTIFICATE OF SERVICE

This is to certify that on December 19, 2008, a true and correct copy of the above and foregoing document was served on Steve Sucsy, Assistant U.S. Attorney, by facsimile transmission to 806.472.7394.

Samuel Mehaffey

CERTIFICATE OF CONFERENCE

I certify that I conferred with Steve Sucsy, the Assistant U.S. Attorney assigned to this matter, regarding the foregoing and does oppose said motion.



Samuel Mehaffey

AFFIDAVIT OF SPECIAL AGENT GARY W. MACNOLL
IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Gary W. Macnoll, being first duly sworn, depose and say:

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI"), United States Department of Justice, and I have been so employed for 25 years. I have been assigned to the Abilene, Texas, Resident Agency since 1983.

2. As part of my official duties, I have conducted and participated in investigations relating to the sexual exploitation of children. During these investigations I have observed and reviewed examples of child pornography in various forms of media, including computer media. As part of my duties and responsibilities as an FBI Special Agent, I am authorized to investigate crimes involving the sexual exploitation of children pursuant to Title 18, United States Code, Sections 1466A, 2251, et seq. Section 1466A makes it a federal offense to knowingly produce, distribute, receive, or possess a visual depiction of any kind that (a) depicts a minor engaging in sexually explicit conduct, and is obscene; or (b) depicts an image that is, or appears to be, of a minor engaging in graphic bestiality, sadistic or masochistic abuse, or sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex, and lacks serious literary, artistic, political, or scientific value, if such visual depiction (referenced in (a) or (b), above), has been mailed, or has been shipped or transported in interstate or foreign commerce by any means, including by computer, or was produced using materials that have been mailed, or that have been shipped or transported in interstate or foreign commerce by any means, including by computer. Section 2252(a)(1) makes it a federal offense for any person to knowingly transport or

Exhibit "A"

ship in interstate or foreign commerce by any means, including by computer, any visual depiction if such visual depiction involves the use of a minor engaging in sexually explicit conduct. Section 2252(a)(2) of Title 18 of the United States Code makes it a federal crime for any person to knowingly receive or distribute child pornography that has been mailed, or has been shipped or transported in interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means, including computer, or knowingly reproduce any visual depiction for distribution in interstate or foreign commerce by any means, including by computer, or through the mails. Section 2252(a)(4)(B) of Title 18 of the United States Code makes it a federal crime for any person to knowingly possess one or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported in interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means, including by computer, if (1) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and (2) such visual depiction is of such conduct. Section 2252A(a)(1) and Section 2252A(a)(2)(A) of Title 18, United States Code, make it a federal crime for any person to knowingly mail, transport, ship, receive, or distribute in interstate or foreign commerce, by any means, including by computer, any material constituting or containing images of child pornography.

3. I have gained expertise in the conduct of such investigations through training in seminars, classes, computer labs, and work experience. I have received in excess of 405 hours of training and instruction in the field of investigation of sexual

exploitation of children, including the following:

- FBI Crimes Against Children (CAC) Coordinator's In-Service, FBI Academy, Quantico, Virginia (VA).
- FBI Advanced CAC Coordinator's In-Service, Alexandria, VA.
- FBI CAC Regional Symposiums-Phoenix, Arizona, and San Francisco, California.
- FBI Computer Investigations In-Service, Dallas, Texas.
- FBI "Image Scan" Forensic Software training for Internet child pornography investigations.
- Dallas Crimes Against Children Conference, Dallas, Texas (7 years).
- Preparing and Trying an Obscenity Case In-Service, United States Attorney's Office, National Advocacy Center (NAC), Columbia, South Carolina.
- Investigation and Prosecution of Advanced Child Exploitation Cases In-Service, United States Attorney's Office, NAC, Columbia, South Carolina.
- Access Data Forensic Tool Kit software training, Dallas, Texas.
- Basic Online Technical Skills Class, National White Collar Crime Center, Ames, Iowa.
- FBI Investigative Child Interviewing Training, NAC, Columbia, South Carolina.
- Case Agent ReviewNet Investigative Review (CAIR).
- In August 2008, I also served on the faculty of the Dallas Crimes Against Children Conference, Dallas, Texas. I presented a child sexual exploitation case study to state, federal, and local professionals employed in the fields of law enforcement; prosecution, child protective services, social work, children's advocacy, therapy, and nursing, who investigate the sexual exploitation of children and work directly with child victims of crime.

4. This affidavit is provided in support of an application for a search warrant for the residence of John Alvin Seyffert, located at 609 Yucca Street, Merkel, Taylor County, Texas 79536. Investigative efforts, including physical surveillance, have identified the residence as a single story family dwelling, as more fully described in

Attachment "A" of this affidavit, which is attached hereto and fully incorporated herein by reference.

5. The statements contained in this affidavit are based in part on information provided by Detective Lori M. Rangel, Dallas Police Department, Child Exploitation Unit, Internet Crimes Against Children Task Force (ICAC), Dallas, Texas, and on my experience, training, and background as a Special Agent with the FBI.

6. As more fully described below, I have probable cause to believe that presently and/or at the time of this warrant's execution, property which is evidence relating to the unlawful possession and/or transportation and receipt of child obscenity, child pornography, and child erotica will be found inside the residence described in Attachment "A" of this affidavit. The items I have reason to believe will be found inside the residence constitute evidence of the commission of the crime of certain activities relating to material involving the sexual exploitation of minors, in violation of Title 18, United States Code, Section 2252, and involving material constituting and containing child pornography, in violation of Title 18, United States Code, Section 2252A. I also have reason to believe material will be found in the residence constituting evidence of the commission of the crime of possession, and/or receipt of child obscenity, in violation of Title 18, United States Code, Section 1466A. Such items are evidence, contraband, the fruits of crime and things otherwise criminally possessed, property designed or intended for use or which is or has been used as the means of committing a criminal offense. These items are described in Attachment "B" to this affidavit, which is attached hereto and incorporated herein.

BACKGROUND

7. Pursuant to my knowledge, training, and experience, as well as the training and experience of other law enforcement personnel, I have learned that:

- a) Collectors of child pornography tend to keep their collections. In Chapter Five of a scientific publication entitled Child Molesters: A Behavioral Analysis, written by Kenneth V. Lanning, a Supervisory Special Agent (SSA) of the FBI (retired as of October 2000), Lanning describes several traits and characteristics of collectors of child pornography. Lanning, a recognized expert in the field of behavioral analysis and child exploitation, has over the past 27 years authored numerous articles on the topic of sexual victimization of children and behavioral analysis of child molesters. His work has formed the basis of the behavioral analysis performed by the FBI in child exploitation cases. Lanning repeatedly refers to the fact that collectors of child pornography do not dispose of the pornography and will go to great lengths to maintain possession of their child pornography. Lanning further states that collectors of child pornography place a great deal of importance on their collection and that "no matter how much the pedophile has, he never has enough; and he rarely throws anything away. If police have evidence that a pedophile had a collection five or ten years ago, chances are he still has the collection now- only it is larger." I have attended several of Lanning's training sessions and, in addition, my personal experience in investigating collectors of child

pornography has confirmed Lanning's conclusions, as set out above.

- b) Individuals (pedophiles) whose sexual objects are children, receive sexual gratification and satisfaction from actual physical contact with children and from fantasies involving the use of pictures and or photographic or art medium depicting children. Such depictions range from fully clothed depictions of children engaged in non-sexual activity, to nude or partially nude depictions of children engaged in sexual activity.
- c) Persons who are sexually attracted to children routinely collect sexually explicit materials involving children, such as photographs, magazines, video tapes, books, slides, and computer images, for their own sexual gratification. The most common method of acquiring the material is by downloading the material from the Internet, by use of a computer.
- d) The use of a computer to traffic, trade, and collect child pornography and hardcore pornography is a growing phenomenon. I am aware that an individual familiar with computers can easily utilize the computer's ability to interact with many distant individuals while remaining largely anonymous. This sense of privacy and secrecy, along with the ability to interact with many individuals without risk of easy identification satisfies the needs of individuals who are interested in trafficking, trading, and collecting child pornography.
- e) Pedophiles rarely, if ever, dispose of their sexually explicit material. Those materials are treated as prized possessions by individuals who collect

child pornography. It is further unlikely that the condition of those items depicting the sexual exploitation of children will be altered or damaged from the original condition at the time of receipt based on the desire to keep the items in the original condition. Moreover, taken together, the increased sense of security which a computer affords and the known desire to retain child pornography for long periods of time, provide probable cause to believe that computer images will be retained for as long as other types of child pornography, if not longer. Furthermore, even images which are erased off a computer hard drive often remain on the hard drive in a format that can be recovered during the forensic analysis of the computer.

f) Collectors of child pornography routinely correspond with each other in order to share information and materials. They also share information and experiences about their sexual interest in children as a means of gaining status, trust, acceptance, and/or psychological support to affirm their sexual preference.

g) Collectors of child pornography also collect other written material on the subject of sexual activities with children, which include fantasy, medical, sociological, psychological, and psychiatric writings. Such writings can now be transmitted by computer, as well as through the mail.

h) Collectors of child pornography almost always maintain and possess their materials in a place considered secure, most frequently within the privacy and security of their own homes, and on occasion, physically on

their persons. As discussed above, child pornography images and/or other related materials may also be stored in a computer, which is often protected by passwords and other security devices and measures.

i) I also know that child pornography is not generally available in retail establishments (including adult book stores), even those which offer other explicit materials. Persons who wish to obtain child pornography, do so by ordering it from abroad or by discrete contact with other individuals who have it available themselves. Commercially produced child pornography historically has been, and continues to be to a large extent, a product of foreign distributors, primarily in Europe and Asia. In ordering such material, I am aware that the recipients normally maintain order forms, proof of purchases, correspondence, and records relating to their sources for procuring the child pornography material.

j) Individuals who are involved with child pornography will often collect, read, copy, or maintain numbers or lists of persons who have similar sexual interests. These contacts are maintained as a means of personal referral, exchange, and commercial profit. These names may be maintained in the original publication or mode of receipt, in phone or note books, on scraps of paper, or in computers.

8. Computers and computer technology have revolutionized the way in which individuals interested in child pornography interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). The

photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. There were definable costs involved with the production of pornographic images. To distribute these on any scale required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contacts, mailings and telephone calls.

9. The development of computers has changed this. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

10. Child pornographers can transfer photographs from a camera onto a computer-readable format with a device known as a scanner. With the advent of digital cameras, the images can also now be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world.

11. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

12. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively

secure and anonymous fashion. Individuals who have an Internet account and an Internet based e-mail address must have a subscription, membership, or affiliation with an organization or commercial service which provides access to the Internet. A provider of Internet access and Internet related services is referred to as an Internet Service Provider or ISP. An ISP is a company that provides individuals and other entities with access to the Internet, typically for a fee, through telephone, cable, or satellite connections. One such ISP is America Online LLC (AOL), which is headquartered in New York City, New York. AOL also offers its customers a comprehensive network of services and proprietary community of websites.

13. Individuals can also access their AOL account by using a different ISP (unaffiliated with AOL) and then logging on to their AOL account to surf the web and access AOL's network of services.

14. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including ISPs such as AOL. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

15. I am aware through training and experience that it is common practice for those involved in receiving and distributing child pornography via the Internet to utilize the

e-mail, chat room, and message board services of ISP's such as AOL in committing their crimes.

16. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains peer to peer software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

DEFINITIONS

17. "Child Erotica" is material that is sexually arousing to pedophiles but does not depict minors engaged in sexually explicit conduct. SSA Lanning defines child erotica as follows:

Any material, relating to children, that is sexually arousing to a given individual . . . [s]ome of the more common types of child erotica include photographs that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids."

See Burgess, Ann, Child Pornography and Sex Rings, Ch. 4 authored by Kenneth Lanning, at p. 83 (Lexington books 1984). I have attended seminars at which both Burgess and Lanning have been featured speakers on the topic of child pornography.

18. Title 18, United States Code, Section 2256, et seq., defines, for the purposes of Section 2252 and 2252A, the following terms:

- a. "Minor" means any person under the age of eighteen (18) years.
- b. "Sexually Explicit Conduct" means
 - A) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex;
 - B) bestiality;
 - C) masturbation;
 - D) sadistic or masochistic abuse; or
 - E) lascivious exhibition of the genitals or pubic area of any person.
- c. "Producing" means producing, directing, manufacturing, issuing, publishing, or advertising.
- d. "Visual Depiction" includes undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image.
- e. The term "computer," as used herein, is defined pursuant to Title 18, United States Code, Section 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device."

19. "Child Pornography," as used in this affidavit, in accordance with the definition in Title 18, Section 2256(8), means any visual depiction, including any

photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where-

(A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;

(B) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or

(C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

20. For the purpose of this affidavit, unless otherwise specifically indicated, the term "computer" refers to the box that houses the central processing unit (CPU), along with any internal storage devices (such as internal hard drives) and internal communications devices (such as internal modems capable of sending/receiving electronic mail or fax cards) along with any other hardware stored or housed internally. Thus, "computer" refers to hardware, software and data contained in the main unit. Printers, external modems (attached by cable to the main unit), monitors, and other external attachments will be referred to collectively as peripherals and discussed individually when appropriate. When the computer and all peripherals are referred to as one package, the term "computer system" is used. Information refers to all the information on a computer system including both software applications and data.

21. The term "computer hardware", as used in this affidavit, refers to all equipment which can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data. Hardware includes (but

is not limited to) any data processing devices (such as central processing units, memory typewriters, and self-contained "laptop" or "notebook" computers); internal and peripheral storage devices, transistor-like binary devices, and other memory storage devices, peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); and related communications devices (such as modems, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone generating devices); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (such as physical keys, locks, and dongles).

22. The term "computer software" as used in this affidavit refers to digital information which can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, optical, or other digital form. It commonly includes programs to run operating systems, applications (such as word-processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs.

23. Based upon my knowledge, training and experience, and the experience of other law enforcement personnel, I know that the Internet is a worldwide computer network which connects computers and allows communications and the transfer of data and information across state and national boundaries. Individuals who utilize the Internet can communicate by using electronic mail (hereafter referred to as "e-mail"). E-mail is an electronic form of communication which can contain letter type correspondence and

graphic images. E-mail is similar to conventional paper type mail in that it is addressed from one individual to another and is usually private. E-mail usually contains a message header which gives information about the individual who originated a particular message or graphic, and importantly, the return address to respond to them.

24. Visual depictions and graphic files referred to below are in the form of "computer graphic files". Computer graphic files are photographs or other visual depictions that have been digitized into computer binary format. Once in this format, graphic files can be viewed, copied, transmitted, and/or printed. Computer graphic files are differentiated by the type of format convention by which they were created. Examples of image computer file extensions, which represent different format conventions, are "jpg", "gif", and "art".

25. "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might be static whereby the user's ISP assigns his computer a unique IP address – and that same number is used by the user every time his computer accesses the Internet.

26. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, paintings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic, optical, or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices

such as floppy diskettes, hard drives, CD-ROMs, digital video or versatile disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory cards/sticks, optical disks, flash (thumb) drives, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any electrical, electronic, optical, or magnetic storage device).

27. "URL" or "Uniform Resource Locator" refers to Internet addresses. Each website on the Internet has a unique address called a Uniform Resource Locator, more commonly known as URL.

**SPECIFICS OF SEARCHES AND SEIZURES OF COMPUTER
SYSTEMS**

28. Based upon my knowledge, training, and experience, and the experience of other law enforcement personnel, I am aware that searching and seizing information from computers often requires agents to seize all electronic storage devices (along with related peripherals) to be searched later by a qualified computer expert in a laboratory or other controlled environment. This is true because of the following:

- a. Computer storage devices (like hard drives, diskettes, tapes, laser disks, CD-ROMs, DVDs, and Bernoulli drives) can store the equivalent of hundreds of thousands of pages of information. Additionally, a suspect may try to conceal criminal evidence, and he might store criminal evidence in random order or with deceptive file names or deceptive file extensions. This requires searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crime. This

sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this kind of data search on site.

b. Searching computer systems for criminal evidence is a highly technical process, requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password-protected, or encrypted files. Since computer evidence can be vulnerable to inadvertent or intentional modification or destruction (both from external sources and from destructive codes embedded in the system, such as "booby traps"), a controlled environment is essential to its complete and accurate analysis.

29. Based upon my knowledge, training, and experience, consultation with experts in computer searches, data retrieval from computers and related media, and consultations with other agents who have been involved in the search of computers and retrieval of data from computer systems, I know that searching computerized information for evidence or instrumentalities of crime commonly requires agents to seize all of a computer system's input/output peripheral devices, related software, documentation, and

data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. This is true because of the following:

a. The peripheral devices which allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output (or "I/O") devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence contained therein. In addition, the analyst may need the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices. If the analyst determines that the I/O devices, software, documentation, and data security devices are not necessary to retrieve and preserve the data after inspection, the government will return them within a reasonable time.

b. In order to fully retrieve data from a computer system, the analyst also needs all storage devices as well as the central processing unit (CPU). Further, the analyst again needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software that may have been used to create the data (whether stored on hard drives or on

external media) for proper data retrieval.

30. In addition, there is probable cause to believe that the computer and its storage devices, the monitor, keyboard, and modem are all instrumentalities of the crimes of receipt and possession of child pornography and child obscenity, in violation of law, and should all be seized.

THE INVESTIGATION- FACTUAL BACKGROUND

31. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause that violations of Title 18, United States Code, Sections 1466A, 2252, and 2252A have been committed, and that

a) property that constitutes evidence of the commission of a criminal offense;

b) contraband, the fruits of crime, and things otherwise criminally possessed; and

c) property designed and intended for use and which has been used as a means of committing a criminal offense,

is located at the residence of John Alvin Seyffert, described in Attachment "A" to this affidavit. The property to be seized pursuant to this warrant is described in Attachment "B" to this affidavit.

32. On December 8, 2007, AOL intercepted an e-mail routed through its central computer system servers after determining the e-mail appeared to have an image of child pornography included with the e-mail (as an attachment or as an embedded image).

33. AOL has developed an internal program for identifying e-mails sent through its system that may contain images of child pornography. If the program finds e-mail that appears to contain an image of child pornography, the e-mail is intercepted while in the process of being transmitted and AOL makes notification to the National Center for Missing and Exploited Children (NCMEC) in accordance with Federal law which requires ISPs to report incidents of child pornography to the NCMEC *CyberTipline*.

34. AOL reported its interception of this particular e-mail to the NCMEC *CyberTipline* and advised this particular e-mail had been sent by an AOL customer with the screen name of "abitex22" while using the e-mail address "abitex22@aol.com". AOL reported that five separate e-mails were transmitted through the AOL system on December 8, 2007 by AOL user "abitex22". AOL further reported to NCMEC that AOL user "abitex22" provided AOL with a billing zip code of 79536 which was determined to be associated with the city of Merkel, Texas.

35. NCMEC forwarded the Cybertip to the Dallas ICAC where it was assigned to Detective Rangel. The information provided by AOL to NCMEC included a copy of the files/video clips that were attachments to the above e-mails. One of the videos depicts two prepubescent boys who are naked and appear to be approximately 8-11 years old. The boys are engaged in genital/anal sexual intercourse. I have also viewed this video clip and I believe the video clip contains visual depictions of minors engaging in sexually explicit conduct.

36. Detective Rangel prepared an affidavit in support of a search warrant to be served on AOL in Virginia where AOL was headquartered at the time. AOL has since

moved its headquarters to New York City. The affidavit was transmitted to the Loudoun County Sheriff's Office (LCSO), Loudoun County, Virginia. Based on Detective Rangel's affidavit and other information, the LCSO obtained a Commonwealth of Virginia search warrant which was served on AOL. On January 2, 2008, Detective Rangel received the results of the search warrant.

37. The information received consisted of images, e-mails, and IP log connections for the account which was created on May 2, 1999. The master screen name for the account was "jseyffert" and the account was registered to John Seyffert, service address of 609 Yucca Street, Merkel, Texas 79536. The account is paid by credit card in the name of John Seyffert. The account also included other screen names associated with the account including the screen name of "abitex22."

38. IP connection data for the period September 29, 2007 through December 8, 2007 revealed the subscriber was accessing the AOL account through IP address 207.155.43.127.

39. Detective Rangel used a forensic tool in order to determine which Internet Service Provider (ISP) held the registration on the IP address 207.155.43.127. The query revealed that the IP address 207.155.43.127 resolved (is registered) to Windstream Communications. Results from an administrative subpoena served on Windstream Communications for the date and time the video clips were downloaded revealed that the IP address was assigned to the account of John A. Seyffert, 609 Yuca [sic] Street, Merkel, Texas 79536, billing telephone (325) 928-5093, alternate billing telephone (325) 928-5573.

The information received also revealed the account utilizes a high speed DSL connection to access the Internet.

40. I have reviewed the results of the AOL search warrant and determined there were numerous images and video clips of child pornography stored in "abitex22"s read and sent folders in his AOL account. What I observed included minor age males engaged in oral-genital and genital-anal sexual intercourse.

41. On August 21, 2008, Bob Jones, Chief of Police, Merkel, Texas, determined through the Merkel City Hall that John Seyffert currently has water utility service at 609 Yucca Street, Merkel, Texas.

42. On August 21, 2008, I drove by the Seyffert residence and observed an individual watering his yard who I believe to be John Alvin Seyffert based on a review of his Texas drivers license photograph. I also observed several vehicles parked at the residence which were determined to be registered to Seyffert. One vehicle, a gray 98 Dodge passenger vehicle, Texas registration 032 HWR, was determined to be registered to Chad Bradshaw at that address.

43. A drivers license query through the Texas Department of Public Safety (DPS) revealed John Alvin Seyffert currently holds Texas drivers license(TDL) # 04490006, expiration date 2013. John Alvin Seyffert is described as a white male, 6' 1', 200 pounds, Date of Birth (DOB) November 4, 1941, home address: 609 Yucca, Merkel, Texas 79536.

44. A query through DPS revealed Robert Chad Bradshaw currently holds Texas ID card # 22040446, expiration date 2010. Bradshaw is described as a white male, 5'11", 160 pounds, DOB September 30, 1985. It should be noted that Bradshaw has been 22

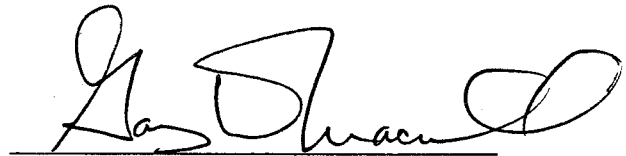
years of age since September 30, 2007 and the screen name "abitex22" is associated with the distribution and receipt of child pornography in this investigation. It has been my experience that Internet users often include personally identifiable information such as their age or their hobby when composing a screen name.

CONCLUSION

45. Based upon all of the information set forth in this application, I respectfully submit that there is probable cause to believe that John Alvin Seyffert, Robert Chad Bradshaw, or an individual using a computer at 609 Yucca Street, Merkel, Texas 79536, is a collector of child pornography, such that this individual is likely to maintain a collection of child pornography and rarely dispose of it. Further, I respectfully submit that there is probable cause to believe that Seyffert, Bradshaw, or another individual, using a computer located at 609 Yucca Street, Merkel, Texas 79536, violated Title 18, U.S.C., Sections 1466A, 2252, and 2252A, by transmitting, receiving and possessing child obscenity and child pornography, and that evidence of these crimes is located at 609 Yucca Street, Merkel, Texas 79536.

46. In consideration of the foregoing, I respectfully request that this Court issue an order authorizing the search of 609 Yucca Street, Merkel, Texas 79536, more fully described in Attachment "A" of this affidavit, including any external storage structures and vehicles under the control of John Alvin Seyffert, Robert Chad Bradshaw, and/or any other individuals located on the property, and any computers and associated devices contained therein, for the items, materials, and records more specifically identified in Attachment "B".

FURTHER AFFIANT SAYETH NOT



Gary W. Macnoll
Special Agent
Federal Bureau of Investigation
Abilene, Texas Resident Agency

SUBSCRIBED TO AND SWORN TO
BEFORE ME THIS 28th DAY OF August, 2008



PHILIP R. LANE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT "A"
DESCRIPTION OF PREMISES TO BE SEARCHED

The property, together with curtilage and vehicles, located at 609 Yucca Street, Merkel, Texas 79536. The property is on the East side of Yucca Street, the second house South of where Yucca Street intersects with South 6th Street.

The property is a single-wide, mobile home, gray in color, with a grey asphalt shingle roof. The front door faces West. A covered porch is located near the front door and the numbers "609" are located on a post supporting the porch. A white unmarked metal mailbox is located in the front yard near the street. A two-car carport is located near the South side of the home. A portable (metal frame, fabric covered) one-car carport is located near the North end of the home.

ATTACHMENT "B"
LIST OF ITEMS TO BE SEARCHED FOR AND SEIZED

This affidavit is in support of an application for a warrant to search the premises known as 609 Yucca Street, Merkel, Texas 79536, which is more specifically identified in Attachment "A," including any computers, associated storage devices and/or other devices located therein that can be used to store information and/or connect to the Internet, for records and materials evidencing a violation of Title 18, United States Code, Sections 1466A, 2252, and 2252A, which criminalizes, in part, the possession, receipt and transmission of child obscenity and child pornography (defined in 18 U.S.C. § 2256), as more specifically identified below:

1. Any and all tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, scanners, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, tape systems, hard drives, terminals (keyboards and display screens) and other computer related operation equipment, in addition to computer photographs, digital graphic file formats and/or photographs, slides or other visual depictions of such digital graphic file format equipment that may be, or are, used to visually depict child obscenity, child pornography, child erotica, information pertaining to the sexual interest in child pornography, sexual activity with children, or the distribution, possession, or receipt of child obscenity, child pornography, or child erotica.

2. Any and all computer software, including programs to run operating systems, applications (like word processing, graphics, or spreadsheet programs), utilities, compilers,

interpreters, and communications programs, including, but not limited to, America Online (AOL) and P2P software.

3. Any computer-related documentation, which consists of written, recorded, printed or electronically stored material that explains or illustrates how to configure or use computer hardware, software or other related items.

4. Any and all records and materials, in any format and media (including, but not limited to, envelopes, letters, papers, e-mail, chat logs and electronic messages), pertaining to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256.

5. In any format and media, all originals, copies, and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256, child erotica, or child obscenity.

6. Any and all records and materials, in any format and media (including, but not limited to, envelopes, letters, papers, e-mail, chat logs, and electronic messages) identifying persons transmitting through interstate or foreign commerce, including via computer, any visual depiction of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256, child erotica, or child obscenity.

7. Any and all records and materials, in any format and media (including, but not limited to, envelopes, letters, papers, e-mail, chat logs, electronic messages, other digital data files and web cache information), bearing on the receipt, shipment, or possession of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256, child erotica, or child obscenity.

8. Records of communication (as might be found, for example, in digital data files) between individuals concerning the topic of child pornography, the existence of sites on the Internet that contain child pornography, or that cater to those with an interest in child pornography, as well as evidence of membership in online clubs, groups, services, or other Internet sites that provide, or make accessible, child pornography to its members and constituents.

9. Evidence of association, by use, subscription, or free membership, with online clubs, groups, services, or other Internet sites including but not limited to AOL, that provide, or otherwise make accessible, child pornography.

10. Evidence of any online storage, e-mail, or other remote computer storage subscription, to include unique software of such subscription, user logs, or archived data that show connection to such service, and user login and passwords for such service.

11. Records evidencing occupancy or ownership of the premises described above, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence.

12. Records, in any format or media, evidencing ownership or use of computer equipment and paraphernalia found in the residence to be searched, including, but not limited to, sales receipts, registration records, records of payment for Internet access, records of payment for access to newsgroups or other online subscription services, handwritten notes, and handwritten notes in computer manuals.

13. The contents of any computer files located on any computer hard drive or any other form of computer storage media, depicting any child engaged in sexually explicit

conduct, depicting any child obscenity or child erotica, or relating to the collecting, receipt, or distribution of any such images.

14. Any and all diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by the operator of by use of the computer or by other means for the purpose of distributing or receiving child obscenity or child pornography as defined in 18 U.S.C. Section 2256(8) or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. Section 2256(2).

AFFIDAVIT OF JASON ALAN SEYFFERT

STATE OF TEXAS

§

COUNTY OF TAYLOR

§

§

BEFORE ME, **JASON ALAN SEYFFERT**, the undersigned authority, on this day personally appeared and after being duly sworn stated under oath:

I.

I am JASON ALAN SEYFFERT. I am over 18 years of age, and I am fully competent and have personal knowledge of the matter set forth herein.

II.


The computer that was seized by federal agents on August 29, 2008 was located in my bedroom. I used my computer to send and receive emails that I assumed were private in nature and I assumed that only the recipients of these emails would be receiving and reading these emails. The AOL email account was in my father's name and I had never read the service agreement and therefore never gave consent to have my emails searched or read by anybody other than the recipient.

III.

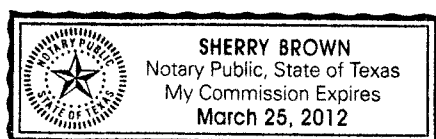
On August 29, 2008, when federal agents, local police, and sheriff's department raided my home, I never felt I had the option to leave my home and certainly was not told that I could leave my home. At no point did I feel like I was free to go nor do I believe a reasonable person would feel like I was free to go.

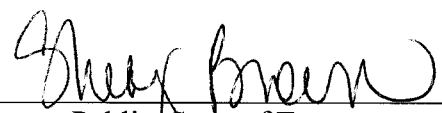
IV.

Agent McNoll is the one that suggested that I go to the police station for the interview. It was not my idea to go to the police station for the interview.


JASON ALAN SEYFFERT

SUBSCRIBED AND SWORN TO BEFORE ME on December 19, 2008.




Notary Public, State of Texas